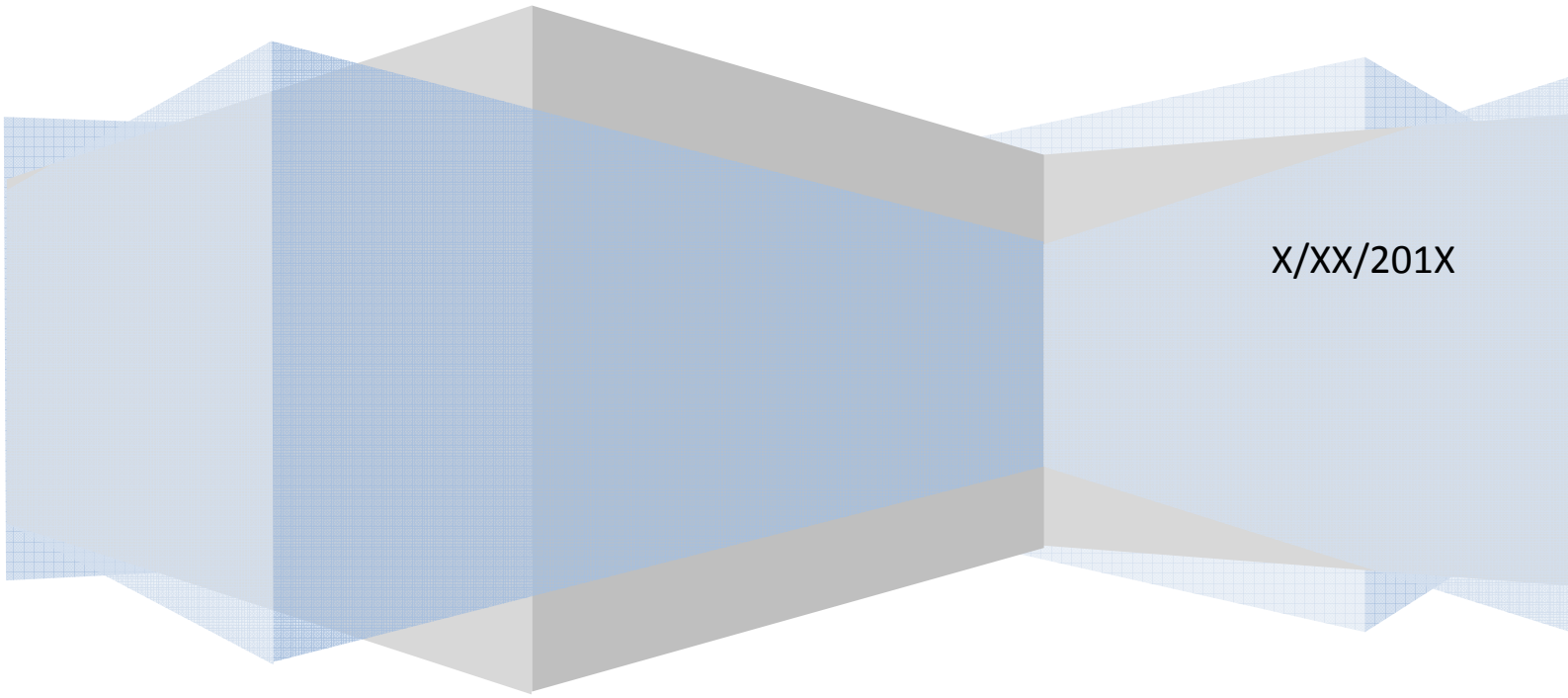
LOGO DELL'AMMINISTRAZIONE

Piano di Continuita' Operativa ICT

Esempio di modello generale



X/XX/201X

F I R M E			
	Unità/Ruolo	**Nominativo**	**Firma**
PREPARATO DA:			
CONTROLLATO DA:			
APPROVATO DA:			
AUTORIZZATO DA:			

LISTA DI CONDIVISIONE:

Nominativo	Unità/ Ruolo	Firma

ELENCO DI DISTRIBUZIONE:

Nominativo	Unità

REGISTRO DELLE MODIFICHE		
EDIZIONE	**SINTESI DELLA MODIFICA**	**DATA**

Sommario

NOTA INTRODUTTIVA AL MODELLO

Il Piano di Continuita' Operativa ICT (nel seguito, semplicemente PCO ICT) è un documento complesso, articolato in più sezioni, che può contenere al suo interno documentazione di natura diversa come procedure operative, organizzative, schede, elenchi di persone e di materiale, istruzioni operative, eccetera.

L'eventuale documentazione a completamento del presente documento deve essere predisposta secondo un criterio di facile reperibilità.

Una tabella riassuntiva di tutta la documentazione può aiutare al reperimento facile ed immediato della documentazione da includere o allegare al PCO ICT.

E' di fondamentale importanza che tutta la documentazione relativa al PCO ICT sia stata gia' approvata dalla dirigenza dell'Amministrazione, soprattutto la documentazione che conferisce gli opportuni poteri e responsabilita' alle varie figure (Comitato di crisi ICT e Responsabile della Continuita' Operativa ICT) durante la fase di emergenza.

Il PCO ICT si compone di attività e fasi che devono essere dettagliatamente specificate e descritte. É utile in ogni caso avere una visione complessiva dell'intero flusso di attività in modo che ciascun soggetto coinvolto abbia immediatamente evidenza delle interazioni tra le singole fasi.

Il PCO ICT rappresenta pertanto una guida generale che indica come reagire ad eventi "negativi" di significativa rilevanza, che determinano l'indisponibilità di quei processi/servizi critici di cui si garantisce il ripristino entro determinati limiti di tempo.

Il PCO ICT prevede l'esecuzione di chiare ed efficaci azioni (formalizzate in procedure, istruzioni operative, atti e documenti), da parte dei soggetti coinvolti nel piano, come completa risposta alla situazione d'emergenza, all'eventuale stato di emergenza, e sono finalizzate al ripristino dei servizi sino al rientro alla situazione di normalità.

Tali azioni dovranno essere eseguite da ciascun soggetto con immediatezza, in considerazione degli obiettivi da perseguire. Inoltre, nell'ambito della struttura organizzativa per il PCO ICT predisposta da codesta Amministrazione il Responsabile della Continuita' Operativa ICT assume un ruolo strategico, sia in condizioni ordinarie sia in eventuali condizioni di emergenza, per assicurare il coordinamento delle operazioni e il mantenimento, aggiornamento e sviluppo futuro del PCO ICT.

1 Obiettivo del Piano di Continuità Operativa ICT

L'obiettivo di questo Piano di Continuità Operativa ICT (nel seguito, semplicemente PCO) è quello di definire organizzazione, procedure, mezzi tecnici che permettano all'Amministrazione di ripristinare, in caso di interruzioni di qualunque natura, i propri servizi, così come definiti nello Studio di Fattibilità Tecnica (nel seguito: SFT) che la stessa Amministrazione ha predisposto e sul quale, così come richiesto al comma 4 dell'articolo 50-bis del CAD, ha ottenuto il parere da parte dell'Agenzia per l'Italia Digitale (nel seguito AID). Il PCO ICT ha la finalità di:

- Gestire un completo e definitivo ripristino dell'operatività in caso di disastro;
- Reagire agli eventi nel modo più tempestivo possibile;
- Stabilire un flusso di comunicazione efficiente in tempi brevissimi in caso di emergenza

Si sottolinea che il Piano oggetto di questo documento si differenzia nelle finalità da altri Piani richiesti dalle normative vigenti, quali:

- Piano di Protezione Civile, secondo Ordinanza del Presidente del Consiglio dei Ministri del 28 agosto 2007, n. 3606,
- Piano di Emergenza, secondo DL 81/2008.

Si precisa, però, che il Piano è stato comunque verificato come coerente con le suddette normative.

Benché il presente Piano rappresenti una specifica realizzazione nel contesto di quanto previsto dall'articolo 50-bis del CAD e non sia, quindi, direttamente riconducibile a un preciso standard, sono norme internazionali di riferimento le seguenti:

- ISO 22301:2012 ("Societal security – Business continuity management systems – Requirements")
- ISO/IEC 27031:2011 ("Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity")
- ISO/IEC 24762:2008 ("Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services")

1.1 Definizioni e abbreviazioni

Terminologia	Acronimo	Definizione
Piano di Continuità Operativa ICT	PCO ICT	Documento operativo che descrive tutte le attività e modalità finalizzate al ripristino, a seguito di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi classificati come "critici"

Terminologia	Acronimo	Definizione
Piano di Disaster Recovery	PDR	Documento operativo che descrive tutte le attività necessarie a garantire, a fronte di un evento negativo di significativa rilevanza, che determini l'indisponibilità dei servizi definiti "critici", il ripristino degli stessi servizi, entro un arco temporale predefinito, tale da rendere, il più possibile, minime le interruzioni nell'erogazione dei servizi. Si evidenzia che il PDR è la sezione del PCO che descrive le attività di ripristino del sistema informativo.

Per ulteriori definizioni di termini ed espressioni che verranno utilizzati, ove non altrimenti specificato, si rimanda al "Glossario" contenuto nelle "Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni".

1.2 Destinatari

Destinatari del Piano di Continuità Operativa ICT sono:

- i vertici dell'Amministrazione;
- il responsabile della CO ICT, così come indicato nelle "Linee guida per il DR delle PA" emesso dall'Agenzia per l'Italia Digitale il 26 novembre 2011;
- il personale dell'Amministrazione di qualunque tipologia (fruitore o gestore) direttamente coinvolto nell'IT dell'Amministrazione;
- la comunità di riferimento territoriale e sociale (cittadini e imprese) dell'Amministrazione;
- le organizzazioni e/o istituzioni che interagiscono con l'Amministrazione in modalità informatiche;
- se presenti, tutti i fornitori, a qualunque titolo, di attività di supporto informatico.

1.3 Il percorso dello Studio di Fattibilità Tecnica ex comma 4, art. 50-bis del CAD

In data ….l'Amministrazione ha presentato richiesta di parere, così come previsto dal comma 4 dell'articolo 50-bis del CAD.

In data ….AID ha emesso parere "favorevole"/"favorevole condizionato".

1.3.1 I servizi in ambito nello SFT

I servizi in ambito identificati nello SFT CON I RELATIVI LIVELLI (Tier) di criticità sono stati seguenti:

Inserire tabella punto 5.2 SFT comprensiva anche di RPO e RTO e senza presenza/assenza soluzione.

L'Amministrazione ha ritenuto, invece, non in ambito, i seguenti servizi:

Inserire tabella con i servizi non ritenuti in ambito

1.3.2 La sintesi del parere di AID.

PQM del parere rilasciato.

1.3.3 Variazioni eventuali nel numero dei servizi e relative criticità.

Inserire la tabella punto 5.2 SFT con aggiunte/modifiche o indicazione di "nessuna variazione"

1.4 Sintesi di informazioni organizzative e tecniche sull'Amministrazione

1.4.1 Matrice servizi/organizzazione (responsabilità)

In questo paragrafo devono essere individuati, sulla base dei servizi facenti parte del perimetro del piano della continuità operativa, l'ufficio responsabile, il nome del responsabile della erogazione del servizio stesso.

SERVIZIO	UFFICIO RESPONSABILE	RESPONSABILE
A		
B		
….		

1.4.2 Matrice servizi/infrastruttura tecnologica

Per ogni servizio deve essere indicato:

- *Nel campo "Sistema(i) di esercizio"*
  - *se il servizio è esternalizzato, oppure*
  - *se il servizio è interno all'amministrazione, nel qual caso vanno indicati in modo puntuali i sistemi hw e sw che rendono operativo il servizio;*
- *Nel campo "Localizzazione" il luogo fisico in cui risiedono i sistemi che concorro alla erogazione del servizio;*
- *Nel campo "LDS" le clausole contrattuali previste per la prestazione del servizio se in carico ad un fornitore, altrimenti gli obiettivi di prestazione del servizio in termini di orario durante il quale deve essere assicurata l'erogazione del servizio.*

In caso di servizio composto da più servizi devono essere chiaramente riportate le relazioni tra i servizi: ogni servizio componente dovrà rientrare nell'ambito di applicabilità del PCO ICT.

SERVIZIO	SISTEMA(I) DI	LOCALIZZAZIONE	LDS (orario

	ESERCIZIO		disponibilità)
A			
B			
….			

2 Predisposizione all'emergenza

In questo capitolo deve essere descritta la struttura organizzativa preposta per il PCO ICT con l'attribuzione di ruoli e responsabilità alle singole risorse coinvolte nel Piano, le liste di reperibilità e contatti.

2.1 La struttura organizzativa

2.2 Comitato di crisi ICT

2.3 Responsabile della Continuità Operativa ICT

2.4 Strutture tecniche

Se esistenti

2.5 Composizione, ruoli, procedure operative

2.6 Gestione delle reperibilità

Reperibilità del comitato gestione di emergenza e dei soggetti coinvolti nelle operazioni di ripristino dei servizi

3 Soluzione di continuità

*I paragrafi che seguono devono essere redatti per **ogni servizio in ambito** (dopo la revisione iniziale dei servizi e le eventuali variazioni – punto 1.3.3). Se le caratteristiche organizzative, procedurali e tecniche sono comuni a più servizi, i contenuti che seguono andranno riferiti a tutti questi servizi, indicandoli nell'intestazione.*

3.1 Interrelazioni del servizio/i con entità esterne all'Amministrazione

Per ogni entità coinvolta devono essere descritte le interrelazioni col servizio A e come queste entità possono condizionare e/o essere coinvolte in caso di disastro (altre PA, fornitori, compagnie di assicurazioni, ecc.).

ENTITA'	DIREZIONE FLUSSI

3.2 Dati logistici generali

Contiene dati quali:

- *dove andare (ubicazione del sito alternativo);*
- *come si accede al sito (percorsi stradali, ferroviari,; parcheggi; ecc.);*
- *autorizzazioni necessarie per accedervi;*
- *….*

Nel caso di servizio esternalizzato dei paragrafi che seguono vanno redatti solo i paragrafi "Posti di lavoro" e "SLA o accordi di servizio specifici"

Dati infrastrutturali

Contiene dati relativi alla esatta localizzazione fisica e impiantistica nella quale è esercita la soluzione per il/i servizio/i in questione.

3.3 Dati logistici specifici

Contiene dati relativi alla precisa localizzazione, all'interno del sito alternativo, dell'ambiente nel quale è esercita la soluzione di continuità.

3.4 Infrastrutture di continuità e protezione fisica

Contiene dati relativi alla localizzazione del punto precedente o all'intera infrastruttura del sito alternativo, punto quali:

- *caratteristiche sistemi di alimentazione e di continuità elettrica;*
- *caratteristiche sistemi di raffreddamento;*
- *caratteristiche sistemi antincendio e antifumo;*
- *caratteristiche sistemi anti allagamento;*
- *…..*

3.5 Controllo fisico degli accessi (impianti e procedure)

Contiene dati relativi alle modalità di accesso fisico (tornelli, porte ad accesso controllato, ecc.) e relative procedure di gestione e ai sistemi di videosorveglianza e relative procedure all'area del sito alternativo (o all'intero sito alternativo) dedicata alla soluzione di continuità.

3.6 Ambiente logistico (interno) per la continuità

Contiene dati sugli asset disponibili presso il sito alternativo (uffici, sale riunioni, impianti di fonia, aree per le postazioni di lavoro, ecc.).

3.7 Apparati hw e postazioni di lavoro

Descrizione delle risorse elaborative e di storage dedicate alla soluzione. Contiene anche le caratteristiche delle postazioni di lavoro (numero, tipologia, procedure per la gestione in caso di normalità e in caso di emergenza, ecc.) Nominativo del fornitore/i dell'assistenza e relativi SLA.

Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

3.8 Sw ambiente

Descrizione del sw di ambiente (sistema operativo, ambiente DB, ecc.). Nominativo del fornitore/i dell'assistenza e relativi SLA.

Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

3.9 Sw applicativo

Descrizione delle applicazioni che supportano la soluzione di continuità. Nominativo del fornitore/i dell'assistenza e relativi SLA.

Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

3.10 Rete interna

Descrizione della rete interna (cablaggio, router, switch, firewall, ecc.). Nominativo del fornitore/i dell'assistenza e relativi SLA.

Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

3.11 Rete esterna

Descrizione dei collegamenti geografici (caratteristiche, fornitore,SLA, ecc.).

Nel caso di risorse non disponibili, in base alla soluzione di continuità scelta, è necessario esplicitare anche le modalità e i tempi di approvvigionamento e operatività delle risorse.

3.12 Istruzioni operative di start up dei servizi

Contiene le indicazioni per:

- *l'attivazione dei sistemi hw e sw dedicati alla continuità;*
- *l'attivazione operativa del servizio/i.*

3.13 Gestione dei sistemi hw, sw, di rete in situazione di normalità

Contiene la descrizione dell'impiego e della gestione dei sistemi dedicati alla soluzione in caso di normalità.

Dati procedurali

Contiene dati relativi alle fasi e alle procedure impiegate per la soluzione di continuità del servizio/i in caso di emergenza.

3.14 Scenari di emergenza applicabili

In questo capitolo verranno riportati un riassunto degli scenari individuati durante lo studio di fattibilita' con i relativi RTO e RPO.

3.15 Fase di reazione all'emergenza

Le attività previste dal PCO ICT in caso di "reazione" ad un evento negativo di portata "disastrosa" rientrano in quello che si definisce "Processo di reazione all'emergenza".

La descrizione dettagliata delle attivita' che compongono tale Processo sono parte preponderante del PCO ICT poiché descrivono "chi fa cosa" dal momento della Reazione all'emergenza fino al Ritorno allo Stato di Normalità.

In questa fase si raccolgono le segnalazioni di incidente. Ciascun evento deve essere analizzato e in caso di gravita' deve essere informato il Responsabile della Continuita' Operativa che ne esamina la criticità e ne stima la gravità. Sarà suo compito valutare se l'evento è tale da generare una possibile situazione di emergenza e, quindi coinvolgere il Comitato di crisi ICT, oppure se l'evento va gestito con le "normali" procedure di gestione degli incidenti.

In questa fase il Comitato di crisi ICT sancisce ufficialmente l'entrata nello Stato di Emergenza e deve essere previsto l'invio delle diverse notifiche ai vertici dell'Amministrazione, al personale dell'Amministrazione, ai fornitori e agli altri soggetti che si ritiene opportuno coinvolgere. Le notifiche inviate ai Team di ICT costituiranno l'avvio ufficiale delle operazioni di riattivazione e rientro. Devono essere inoltre descritte in questo capitolo le modalità alternative di comunicazione da adottare nel caso in cui la modalità primaria non sia disponibile.

Nel corso di questa fase è inoltre necessario provvedere tempestivamente alla reazione all'emergenza stessa e per questo motivo è necessario definire le diverse modalità di escalation da seguire a fronte di specifici eventi negativi.

I passi da seguire sono:

- *Segnalazione dell'emergenza*
- *Valutazione della criticità*
- *Attivazione del comitato gestione della crisi ICT*
- *Modalità di gestione dell'emergenza, che contiene dati quali:*
    - *trasferimento del personale;*
    - *occupazione del sito alternativo;*
    - *innesco del piano di DR;*
    - *chi deve andare a casa e chi deve trasferirsi nel sito alternativo,*
    - *cosa deve fare il personale presso il sito alternativo,*
    - *cosa non deve fare il personale presso il sito alternativo,*
    - *…..*

3.16 Fase di gestione dell'emergenza e riattivazione dei servizi

Le attività prioritarie, successivamente alla notifica dello stato di emergenza, sono comunque quelle di ripristino dei servizi sul sito secondario di Disaster Recovery. Devono quindi essere descritte le procedure che il Team di ICT dovrà eseguire per lo start-up dei sistemi e verifica degli allineamenti (dichiarando così il momento a partire dal quale si sono persi i dati) e di attivazione e test di tutti i servizi in DR. Infine, successivamente alla dichiarazione di "sistemi up & running", deve essere definito come notificare il passaggio sul sito secondario (tale notifica è necessaria per la verifica del rispetto del parametro di RTO). Durante lo Stato di emergenza è probabile che sia necessario operare utilizzando modalità alternative anche per le attività di acquisto di materiale/strumenti e/o di gestione delle trasferte dei dipendenti. Per queste finalità è necessario quindi redigere delle procedure specifiche. Dovranno infine essere previste procedure per la comunicazione verso il personale, i soggetti terzi coinvolti ed eventualmente i media.

I passi da seguire sono:

- *Modalità di dichiarazione dello stato di emergenza*
- *Comunicazione al personale (reperibile, altro personale)*
- *Comunicazione ai mezzi di comunicazione e ai soggetti terzi sullo stato di emergenza*
- *Modalità di notifica all'azienda (fornitore) che ha stipulato il contratto di fornitura di servizi per il DR*
- *Dichiarazione servizi attivi su sito di DR*

3.17 Fase di ritorno alla normalità

In questa fase è necessario valutare le possibili strategie di rientro e scegliere se rientrare sul sistema primario oppure promuovere il sito secondario a primario. Vista la natura strategica della scelta è necessario il coinvolgimento del Comitato di crisi ICT. In funzione della strategia individuata il personale ICT si adopererà per garantire il rientro sul primario o sul secondario (che diventa primario) con livelli di performance normali. Al termine una fase di test verificherà che il rientro sia avvenuto in maniera efficace. Una notifica formale decreterà il rientro alle condizioni di normale operatività. Dovrà poi essere prevista una attività di reportistica per registrare quanto accaduto ed analizzarlo successivamente per valutare l'efficacia del PCO ICT ed eventualmente provvedere al suo aggiornamento.

I passi da seguire sono:

- *Analisi dei danni*
- *Organizzazione e pianificazione delle attività di rientro*
- *Reportistica (descrizione emergenza, descrizione test di verifica rientro)*

4 Formazione

La formazione delle risorse riveste un ruolo fondamentale per assicurare la corretta applicazione, conoscenza e padronanza del Piano. Periodicamente è necessario verificare il livello di formazione di tutte le risorse coinvolte nel PCO ICT affinché ciascuna sia ben consapevole delle attività da svolgere in caso di Emergenza. Tutte le risorse coinvolte nel PCO ICT devono essere formate ed istruite circa l'applicazione delle procedure e modalità da seguire nelle diverse attivita' sia ordinarie sia di emergenza. E' compito del Responsabile della Continuita' Operativa ICT assicurare un'efficace pianificazione della formazione sia in termini di periodicità sia di contenuti.

I passi da seguire sono:

- *Redazione del piano di formazione*
- *Redazione del programma di formazione*
- *Test per la valutazione del livello di conoscenza del Piano*
- *Relazione di sintesi dei risultati dell'attività formativa*

5 Gestione e aggiornamento del piano di continuita' operativa

Il PCO ICT non è un documento statico e, pertanto, è necessario pianificare, all'interno del PCO ICT stesso, sia le modalità di verifica dei contenuti (test), sia le modalità di revisione e aggiornamento.
Per quanto attiene ai test, sono possibili varie modalità di test:

- *una semplice verifica dell'effettiva disponibilità di tutto quanto si renderebbe necessario in caso di emergenza (nomina responsabile CO, nomina Comitato di crisi ICT, gestione delle reperibilità, disponibilità e funzionamento degli impianti del sito secondario, disponibilità delle risorse elaborative e di rete, ecc.). In questo caso va preventivamente predisposta una cheklist che*

permetta di verificare quanto sopra. Questo tipo di test non garantisce che in caso di emergenza non ci siano funzionalità non in linea con quanto previsto, ma è facilmente eseguibile;

- *un test cosiddetto "walkthrough": questo tipo di test si svolge con una simulazione (cioè, senza attivazione fisica dei sistemi) fatta da tutto il personale da coinvolgere previsto dal PCO ICT. Deve essere preparato con cura, soprattutto per descrivere lo scenario di crisi ipotetico verso il quale ciascun partecipante, secondo il ruolo che ha nel PCO ICT, esegue le procedure previste per ognuna delle fasi indicate. Anche se più complesso da organizzare rispetto alla semplice verifica della disponibilità di risorse e impianti, questo test non implica l'attivazione dei sistemi alternativi e può essere un modo utile anche per la formazione e la verifica della preparazione del personale;*
- *test degli impianti e delle risorse: in questo caso non solo le procedure, ma anche l'effettiva attivazione delle risorse fisiche e IT viene verificata, sempre a fronte della simulazione di un'emergenza. Un test di questo tipo richiede una attenta predisposizione e un sensibile impegno per il personale, ma garantisce la reale verifica della soluzione di continuità del PCO ICT. Per ognuna delle fasi dell'emergenza vanno programmate ed eseguite le attività previste.*

Collegato al tipo di test degli impianti, è il test effettuato senza preavviso delle risorse interessate. Si tratta di una possibilità realmente fattibile solo in presenza di una alto livello di professionalità delle figure coinvolte. Naturalmente, un simile test si avvicina a quanto effettivamente potrebbe prodursi in caso di emergenza e permette un livello di garanzia della funzionalità della soluzione di continuità estremamente alto.
E' necessario, al minimo, eseguire almeno un test all'anno.

Quanto all'aggiornamento e alle revisioni da fare per il PCO ICT, vanno segnalate nello stesso le condizioni ordinarie che si possono verificare determinando cambiamenti organizzativi, tecnici, logistici, procedurali che hanno effetti rilevanti su una o più parti del Piano.
A titolo di esempio si riportano di seguito alcune tipologie di eventi che devono essere presi in considerazione per l'adeguamento del PCO ICT:

- *modifiche nella composizione della/e struttura/e organizzava/e (Comitato di gestione della crisi ICT, resp. CO ICT, gruppi di supporto, ecc.) preposte alla gestione della continuità operativa ICT;*
- *modifiche nei dati personali e/o di reperibilità;*
- *modifiche dei fornitori e/o del contratto assicurativo;*
- *modifiche dei servizi o delle applicazioni software (aggiunta o eliminazione di applicazioni, variazioni nella criticità delle applicazioni);*
- *modifiche nell'hardware e/o nella rete;*
- *modifiche nella logistica;*
- *stipula di nuovi contratti.*

Il verificarsi di uno di questi eventi, o comunque di un qualsiasi evento che può incidere sull'efficacia del PCO ICT, richiede quindi un'attenta analisi per valutare la necessità di attuare delle modifiche al Piano, cioè di un suo adeguamento.

E' comunque necessario che almeno una volta all'anno, in concomitanza o meno con il test, il Comitato di crisi si riunisca per analizzare la completezza e attualità del PCO ICT.

I settori nel PCO ICT che danno evidenza di queste attività sono i seguenti:

5.1 Modalità di esecuzione dei test periodici

5.2 Modalità di revisione e adeguamento del piano